# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 03-265241
(43)Date of publication of application : 26.11.1991

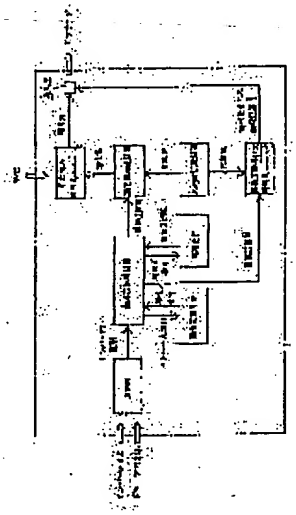
(51)Int.Cl. H04L 9/06
H04L 9/14

(21)Application number : 02-063583
(22)Date of filing : 14.03.1990

(71)Applicant : S R SOKEN KK
MATSUSHITA ATSUSHI
OKADA KENICHI
(72)Inventor : MATSUSHITA ATSUSHI
OKADA KENICHI

## (54) GENERATING METHOD FOR MULTIPLEX KEY AND ITS MANAGEMENT METHOD

(57)Abstract:
PURPOSE: To minimize damage due to leakage of secret information and to simplify and facilitate key management by using a key generating means so as to generate a 2nd key with a 1st key input possessed by each member so as to use it as a communication key thereby decreasing number of keys to be managed.
CONSTITUTION: When a name of a member and a name of a group are entered, the member is identified via an identification list and a key correction processing unit supplies a 1st key possessed by the member and a common key from a common key storage device corresponding to the key and a communication key generator generates a 2nd key. The key is used as a communication key, and as soon as a plain text is encrypted by a cryptographic unit, a header number generated and encrypted similarly is added and the result is outputted as a message. Number of keys to be managed is reduced by the method, the key management is simplified and facilitated and damage due to leakage of secrecy is minimized.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平3−265241

⑤Int. Cl.⁵　識別記号　庁内整理番号　⑬公開　平成3年(1991)11月26日

H 04 L 9/06
9/14

6914−5K　H 04 L 9/02　Z

審査請求　未請求　請求項の数 6　(全11頁)

⑤④発明の名称　多重鍵の生成方法およびその管理方法

⑳特　願　平2−63583

㉒出　願　平2(1990)3月14日

⑦②発明者　松下　温　東京都新宿区喜久井町36

⑦②発明者　岡田　謙一　東京都文京区本郷4−25−12

⑦①出願人　エスアール総研株式会社　東京都千代田区内神田1−15−17

⑦①出願人　松下　温　東京都新宿区喜久井町36

⑦①出願人　岡田　謙一　東京都文京区本郷4−25−12

⑦④代理人　弁理士　鈴木　正次

## 明　細　書

1．発明の名称

多重鍵の生成方法およびその管理方法

2．特許請求の範囲

1　各メンバーが所持する第1の鍵を、鍵生成手段に入力することにより、第2の鍵を生成することを特徴とした多重鍵の生成方法

2　同報通信ネットワークのメンバーが所持する第1の鍵を鍵生成手段に入力することにより、第2の鍵を生成し、第2の鍵を通信用鍵とすることを特徴とした多重鍵管理方法

3　同報通信ネットワークのメンバー表から、各メンバーが持つ共通のピースを求め、このピースとメンバーが所持する共通鍵を鍵生成手段に入力して第1の鍵を生成し、この第1の鍵を鍵生成手段に入力することにより、第2の鍵を生成し、第2の鍵を通信用鍵とすることを特徴とした多重鍵管理方法

4　階層通信グループの夫々のメンバーに配布された第1の鍵と、メンバー毎に定められたピース、又は管理センターから教えられたピース番号から自己保有のピース内より選定したピースを鍵生成手段に入力して第2の鍵を生成し、この第2の鍵を通信用鍵とすることを特徴とした多重鍵管理方法

5　第2の鍵を生成する複数のピースは、階層毎に種類と数を変える手段を付与した請求項4記載の多重鍵管理方法

6　ピースの種類と数は、ラグランジュ補間多項式より求められる曲線上から任意に選択する手段を付与した請求項4記載の多重鍵管理方法

3．発明の詳細な説明

(産業上の利用分野)

この発明は、ユーザーが所有する第1の鍵又は第1の鍵とピースとによって通信用第2の鍵を生成すること、およびこの鍵を通信に使用することを特徴とした多重鍵の生成方法およびその管理方法に関する。

(従来の技術)

現在ＬＡＮや衛星通信を利用したネットワークなどを秘密通信に使用する場合に、同報暗号通信方式としてコピー鍵方式が用いられている。

また多くの組織上の階層構造における秘密通信は、個別通信の暗号方式を拡張使用している。

（発明により解決すべき課題）

然るに、前記コピー鍵方式は、通信性能が優れている反面、ユーザーの保持する鍵の数が多く、鍵配布の複雑性があり、かつグループ構造の変化に対する柔軟性の欠如など鍵管理の面に多大の問題点があった。

また、階層構造通信においては、メンバーの増加に伴い、ユーザーの保持する鍵の数が著しく多くなり、鍵管理面で問題点があり、更に盗難、紛失、漏洩等により盗聴される危険性が大くなるなどの問題点もあった。

（課題を解決する為の手段）

この発明は、メンバーの所持する第１の鍵又はピースによって第２の鍵を生成し、この生成した鍵を通信に使用することにより、前記従来の問題点を解決したのである。

即ちこの発明は、各メンバーが所持する第１の鍵を、鍵生成手段に入力することにより、第２の鍵を生成することを特徴とした多重鍵の生成方法である。また、同報通信ネットワークのメンバーが所持する第１の鍵を鍵生成手段に入力することにより、第２の鍵を生成し、第２の鍵を通信用鍵とすることを特徴とした多重鍵管理方法である。

また他の発明は、同報通信ネットワークのメンバー表から、各メンバーが持つ共通のピースを求め、このピースとメンバーが所持する共通鍵を鍵生成手段に入力して第１の鍵を生成し、この第１の鍵を鍵生成手段に入力することにより、第２の鍵を生成し、第２の鍵を通信用鍵とすることを特徴とした多重鍵管理方法である。

また他の発明は、階層通信グループの夫々のメンバーに配布された第１の鍵と、メンバー毎に定められたピース、又は管理センターから教えられたピース番号から自己保有のピース内より選定したピースを鍵生成手段に入力して第２の鍵を生成し、この第２の鍵を通信用鍵とすることを特徴とした多重鍵管理方法である。

次に、第２の鍵を生成する複数のピースは、階層毎に種類と数を変える手段を付与したものである。更に、ピースの種類と数は、ラグランジュ補間多項式より求められる曲線上から任意に選択する手段を付与したものである。

前記グループ同報通信において、或鍵Ｋを入力の一つとして実際の通信に用いる鍵$K_1$を生成するには次式による。

$$K_1 = f(K, I) \quad \cdots(1)$$

前記において関数ｆは、ＫとＩにより$K_1$を生成する一方向関数、または暗号化関数である。さらに異なるＫ，Ｉに対して、異なる$K_1$を生成できるように、Ｋ空間から$K_1$空間への変換は、１対１の対応、もしくは著しく退化しないことが必要である。またＩは鍵を生成する為の情報であり、関数ｆを暗号化関数とみなした場合の暗号鍵に相当する。

そこで、複数情報$I_1$、$I_2$…Ｉｎにより鍵を生成する場合は、次のように関数ｆを多重に用いる。

$$K_1 = f(\cdots f(f(K, I_1), I_2)\cdots I_n) \quad \cdots(2)$$

前記のようにして鍵の生成法を用いることにより、１個の鍵と情報により複数の鍵を生成することができる。例えば１個の鍵とｎ個の情報から生成される鍵の総数は、ｎ個の情報から$1 \leq r \leq n$をみたすｒ個を選ぶ組み合わせの総数に等しいので、次式のようになることがわかる。

$$\sum_{r=1}^{n} {}_nC_r = 2^n - 1 \quad \cdots(3)$$

従ってユーザーは１個の鍵とｎ個の情報を管理することによって、合計で$2^n$個の鍵を管理することができる。

次に、階層鍵生成方式はラグランジュ補間多項式に基づいて、鍵を分割補間する方法であり、次のような任意の（ｔ－１）次多項式で与えられる。

$$h(X) = (as + a_1X \cdots + a_{t-1}X^{t-1}) \pmod{p} \quad \cdots(4)$$

但し、ｐは大きな素数

前記(4)式で表わされる曲線上に点をばらまき、

それをピースDと名付ける。

$$D_i = n(X_i) \quad (i = 1, 2 \cdots) \cdots (5)$$

但し、$X_1 < X_2 < \cdots$

ピースn個（$n < t$）を任意に選び出し、座標上のそれらn点をつないでできる（n－1）次の曲線g（X）が、ラグランジュ補間多項式より次のように求まる。

$$g(X) = \sum_{s=1}^{n} D_s \prod_{j=1, j\neq s}^{n} \frac{X - X_j}{X_s - X_j} \quad (\mathrm{mod}\, p) \cdots (6)$$

定数値g（0）の値を暗号化し、復号化の時に用いる鍵（K）とする（第1図）。

$$K = g(0) = \sum_{s=1}^{n} D_s \prod_{j=1, j\neq s}^{n} \frac{X_j}{X_j - X_s} \quad (\mathrm{mod}\, p) \cdots (7)$$

第1図の$K_{123}$を使ってかけた暗号文は、ピース$D_1$、$D_2$、$D_3$を持つユーザーだけ読め、2つしかピースを持たないユーザーには読めない。これを階層構造に応用するには、ユーザーが持つピースの種類と数を階層ごとに変えて、例えば第2図のようにする。即ちユーザー$U_1$は部下$U_2$、$U_3$、$U_4$がかけた暗号文は全て読めるが、ユーザー$U_2$、$U_3$、$U_4$は上司$U_1$の暗号文は読めないことになる。前記第2図のような階層構造にするには次のように各ユーザーにピースを配布する。

ピースは必ず2個の組み合わせを最小単位とする。ピース1個では、そのピース自体が鍵となり、安全性が低くなるので前記のようにする。

次に階層構造の基本単位2層の場合を考える。最下層でのピース2個の組合わせを効率よく使い、第2層の人が所持するピース数をなるべく少なくすることを考えると、枝の数Kは、

$$K = mC_2 \quad (m = 3, 4 \cdots) \cdots (8)$$

とすればよいことになる。

前記において、Kはユーザーが適用する階層構造の形態の特徴（段数が多いのか、或いは段数は少ないが下層に広がっているのか等）に合わせて決めれば、いろいろな階層構造に対応できる。

即ち、第3図にはK＝3の場合の例を示す。前記におけるピースの管理は、第4図のように集中管理方法を用いる。即ち、ピースは各ユーザーが保管し、ピース番号を知ることができても、ピース自体を知ったり、直接手を加えたりできないような環境に設定する。そして、ピース番号リストをピース番号管理センターで管理する（第4図）。前記における階層構造においては、同階層への通信はできない。前記方法の安全性は、ピースの完全な秘密保管にかかってくる。鍵が生成されると暗号化は慣用的方法(Data Encryption Standard)で行うので安全である。従ってピースの中味さえわからないような環境を設定すれば、下層が共謀したり、鍵が盗まれても単にピース番号だけで鍵を生成できないので、被害を最小に抑えることができる。

従来用いられているコピー鍵方式の場合は、自分が属するグループの数が処理する鍵の数になる。これに対し、階層構造では縦割のグループとなり、第n段の人が所持する鍵数は、

$$1/2\,(3^n - 3)$$

となる。一方、階層鍵生成方式の場合、第n段の人が所持するピース数は前記第3図から、

$$\begin{cases} 2 & (n = 1) \\ \frac{1}{2}(3^{n-1} + 3) & (n \geq 2) \end{cases}$$

で、$n \geq 2$となれば、階層鍵生成方式の方が所持するものが少なく、（n＝3の時、鍵12、ピースだと6）であり、所持しているのは鍵でなくピースなので、安全性が高いことになる。

次に個別通信は、メンバー数2のグループ内同報通信として扱われる。鍵生成の為の関数fを暗号関数とすると、情報は暗号化の鍵に相当するものになる。そこで1個の鍵とn－1個の情報を保持することは、n個の鍵を保持することと同様である。この発明におけるグループ指向鍵管理方式によれば、従来のコピー方式と同様に、データ長は暗号化の鍵のデータ長と等しくなるので差異はない。

また、この発明によるメッセージnを暗号化または復号化する際の処理時間を従来のコピー鍵方式と比較すると次のようになる。

この発明と、従来のコピー方式とは共に暗号化処理にはDES(5)で代表される慣用暗号系を用いるものとし、また、この発明の関数fにもその暗号系を使用するものとすると次式が成立する。

$$M = K \cdot |K| \quad \cdots (8)$$

但し、|K|は1度に処理されるブロック長または鍵Kのビット長。Kはブロック数。

前記におけるそれぞれの方式の鍵の処理時間を演算回数で表すとすると、コピー鍵方式の演算回数Vcは次式となる。

$$Vc = 3 \cdot K \cdot \log |K| \quad \cdots (10)$$

一方、この発明の演算回数Vgは、

$$Vg = 3 \cdot K \cdot \log |K| + 3 \cdot b \cdot \log |1KG| \cdots$$

$$= 3 \cdot (K + b) \cdot \log |K| \quad \cdots (11)$$

但し、b：多重度（＝n－m）

|1KG|：情報のビット長

となり、前記VcとVgとを比較すると、Vgの方が鍵生成のための処理時間が余分にかかることがわかる。しかし、一般通信において、K＞bであることを考慮すれば、鍵処理時間は無視できる程度であり、この発明の方式の問題点とはならない。

次にこの発明の実施例について説明する。

（実施例1）

次に全同報を除くグループ間同報の暗号化、復号化の手順を述べる。全同報を行う場合は、鍵を生成することなく、共通鍵を用いて暗号化、復号化を行う。

(1) 暗号化

ステップ1　グループのメンバー名よりメンバーが共通に持つ共通鍵（以下ＫＭという）の番号を得る。

ステップ2　ステップ1で求めた番号よりＫＭを得る。

ステップ3　ステップ2で得られたＫＭと共通鍵Ｋ。より通信鍵を生成する。

ステップ4　生成された通信鍵を用いて送信したい平文を暗号化する。

ステップ5　共通するＫＭの番号を共通鍵を用いて暗号化し、ヘッダとして暗号文に付加し、同報通信文を生成する。

これは、受信者にどのＫＭを用いて鍵を生成したかを知らせるためである。同報通信文の構造を第6図に示す。

(2) 復号化

ステップ6　受け取った同報通信文をヘッダと暗号文に分離する。

ステップ7　ヘッダ部を共通鍵によって復号化し、メンバーが共通に持つＫＭの番号を得る。

ステップ8　ステップ7で得られた番号よりＫＭ自体を得る。もし、通信文を受け取ったユーザがその番号のＫＭの一部分しか持っていなければ、次以降のステップには進めない。

ステップ9　ステップ8で得たＫＭと共通鍵より通信鍵を生成する。

ステップ10　暗号文をステップ9で生成した通信鍵を用いて復号化し、平文を得る。

次に暗号化システムについて説明する。

第7図に暗号手順を実現するためのシステムを示す。

まずはじめに、ユーザはグループのメンバー名、またはグループ名を識別表(Identifier Table)に入力する。識別表では、メンバー名やグループ名をメンバーの識別に変換しこれを鍵修正処理装置(Key Modifier Management Unit)に送る。鍵修正処理装置では入力された識別をもとにして、全ユーザ識別と彼らが保持するＫＭの番号が記憶されている鍵修正番号表(Key Modifier Number Table)、またＫＭ自体が記憶されている鍵修正表（Key Modifier Table）を参照して、グループのメンバーに共通するＫＭを出力する（ステップ1、ステップ2）。

通信鍵生成装置（Key Concration Unit）では、共通するＫＭと、共通鍵記憶装置（Common Key Storage)に記憶されている共通鍵より通信鍵を生成する（ステップ3）。

平文用の暗号化ユニット、鍵修正番号用の暗号化ユニット（EnCryption Unit）は、共に暗号化処理部である。平文用の暗号化ユニットでは、生

成された鍵を用いて平文を暗号文とする。鍵修正番号用の暗号化ユニットでは、共通鍵を用いて共通するＫＭの鍵修正番号（Key Modifier Number）を暗号化し、暗号化された鍵修正番号を生成する（ステップ4）。

また、復号化システムは次の通りである。

第８図に復号化手順のためのシステムを示す。

まず、鍵修正用の復号化ユニット（Decryption Unit for KMN)は、分離された暗号化された鍵修正番号を共通鍵を用いて復号化する（ステップ7）。

鍵修正処理装置では、そのＫＭ番号を入力として、鍵修正表を参照することによってＫＭを取り出す。通信鍵生成装置では、暗号化システムと同様にＫＭと共通鍵より通信鍵を生成する（ステップ8）。

平文用の復号化ユニット(Decryption Unit for text)では、通信鍵を用いて暗号文を復号化し、平文を得る。

（実施例２）

次に、多くのグループが形成され、各ユーザーは複数のグループに属しているようなネットワークについて説明する。

同報通信は、グループ内のメンバーで行われる。ネットワーク上にｎ人のユーザーが存在する場合に、情報を次のように分配する。まず、ｎ個の情報（$I_1$、$I_2$ … $I_n$）を用意し、ｎ－１個づつの互いに異なる組み合せに分ける。そこで各ユーザーは共通鍵$K_0$と、前記ｎ－１個の情報の組み合わせの１つを保持する。ここでユーザー$U_1$と$U_3$が共通に持つ情報を考えると、そのような情報はｎ－２個存在し、この組み合わせは、ｉ，ｊによって一意に決まる。そこでメンバー数ｍのグループでは、メンバーであるユーザーが共通に持つ情報はｎ－ｍ個であり、メンバー以外のユーザーはこれらの共通する情報の全てを持っていないことになる。第５図によれば、ｎ＝５の場合に、グループ「$U_1$、$U_3$、$U_4$」のメンバーである$U_1$、$U_3$、$U_4$は$I_1$、$I_4$を共通に保持するが、メンバーでない$U_2$、$U_5$はそれらの何れか１個しか持っていない。

前記において、メンバーが共通に持っている情報を用いて共通の鍵$K_0$より生成した鍵をそのグループの鍵として使用すれば、グループ内での秘密同報通信ができる。然し乍ら、全ユーザーが共通にもっている情報に存在しないので、全同報通信を行うためには、共通鍵$K_0$をそのまま鍵として使用する。また暗号文には、どの情報を用いて暗号に用いた鍵$K_i$を生成したかわかるように情報を管理する通し番号ｉが通信文に付加される必要がある。

前記第５図において、グループ「$U_1$、$U_3$、$U_4$」のグループ鍵$K_{184}$の生成には、次式を用いる。

$$K_{184} = f(f(K_0, I_1), I_4) \quad \cdots (2)$$

前記のように、この発明によれば、ｎ人のユーザーがネットワーク上に存在する環境で、各ユーザーは１個の共通鍵$K_0$と、ｎ－１個の情報を管理するだけで、１対１の通信も含むあらゆるグループ内同報通信を行うことができる。

（実施例３）

(1) 上層から下層のユーザへ送信する場合

○例えば第４図において、$U_1$から$U_2$へ送信する場合

$U_2$は、$U_1$が保持しているピースの一部分を保持しているはずであるが、それが何番のピースであるかは分らない。そこで、センタに問い合わせてピース番号（１、２）を知り、その番号のピース（$D_1$、$D_2$）で鍵を生成し、平文を暗号化して、さらにこれに鍵を生成したピース番号を暗号化された鍵修正番号として付加して、それを通信回線上で送信する。通信文を受信した$U_2$は、暗号化された鍵修正番号から自分のピースから鍵を生成し、その鍵を用いて暗号文を復号化する。具体的には次の３段階の手順を踏む。

(a) センタへの問い合わせ

ステップ１　自分の保持しているピースを全て使用して鍵を生成する。

ステップ２　その鍵を用いて、自分の名前と送信したい相手の名前を暗号化する。

ステップ３　鍵生成に用いたピースの番号を暗

号化された鍵修正番号として暗号化した名前に付加する。

ステップ 4　できあがった通信文を“問い合わせ”としてセンタに送る。

センタでは送られてきた問い合わせを復号化し、2つの名前より共通なピース番号を求め、その番号を暗号化して送信する。

(b)　センタからの回答と暗号

ステップ 5　センタからの“回答”を自分の持っている全てのピースより生成した鍵を用いて復号化し、自分と送信したい相手が共通に持つピースの番号を得る。

ステップ 6　ピース番号よりピース自体を得る。

ステップ 7　ステップ6 で得たピースより鍵を生成する。

ステップ 8　生成した鍵で平文を暗号化する。

ステップ 9　暗号文に、鍵を生成したピース番号を暗号化された鍵修正番号として付加し、通信文とする。

ステップ10　できあがった通信文を送信する。

(c)　復号化

ステップ11　受け取った通信文を暗号化された鍵修正番号と暗号文に分離する。

ステップ12　暗号化された鍵修正番号から共通のピース番号を求める。

ステップ13　ピース番号よりピースを求める。

ステップ14　ステップ13で得たピースを用いて鍵を生成する。

ステップ15　生成した鍵を用いて暗号文を復号化し、平文を得る。

(2)　下層から上層へ送信する場合

o 例えば第４図で$U_2$ から$U_1$ へ送信する場合

$U_2$ が持っているピース（$D_1$、$D_2$）より鍵を生成し、平文を暗号化して通信回線上に流す。同報通信文を受信した$U_1$ は、通信文の暗号化された鍵修正番号よりピース番号を知り、その番号に対応するピースから鍵を生成して、暗号文を復号化する。具体的には次のようになる。

(a)　暗号化

ステップ 1　自分の保持している全ピースより鍵を生成する。

ステップ 2　生成した鍵で平文を暗号化する。

ステップ 3　暗号文に、鍵を生成したピース番号を暗号化された鍵修正番号として付加し、通信文とする。

ステップ 4　できあがった通信文送信する。

同報通信文の構成は、(1)の場合と同様になる。

(b)　復号化

ステップ 5　受け取った通信文を暗号化された鍵修正番号と暗号文に分離する。

ステップ 6　暗号化された鍵修正番号から共通のピース番号を求める。

ステップ 7　ピース番号よりピースを求める。

ステップ 8　ステップ7 で得たピースを用いて鍵を生成する。

ステップ 9　生成した鍵を用いて暗号文を復号化し、平文を得る。

第９図にセンタへ問い合わせるためのシステムを示す。

まずユーザは、送信したい相手の名前、送信相手名(Request User's Name) を送信装置(Request Unit)に入力する。送信装置では、送信相手名を鍵修正番号の暗号化ユニット（EnCryption Unit）に送り、また、自分の持っている全てのピース番号(All Piece Number)をピース処理装置（Piece Management Unit)に送る。全てのピース鍵を入力されたピース処理装置では、ピースが記憶されているピース表（Piece Table ）より、全てのピース(All Piece) を求め、これを通信鍵生成装置（Key Generation Unit)に送る。通信鍵生成装置で生成された全てのピースの番号(All piece Key) は平文用の暗号化ユニットに送られ、ここで送信相手名が暗号化される。この暗号化された通信相手名（CRUN:Ciphered RUN ）には、全てのピース番号が暗号化された鍵修正番号として付加され、問い合わせ文(request) となる。

第１０図には、センタでの処理システムを示す。

センタではまず、受け取った問い合わせを暗号化された鍵修正番号（全てのピース番号）と、暗

号化された共通ピース番号に分離し、全てのピース番号より、前述の方法で鍵を生成する。分離され、暗号化された共通ピース番号と生成された全ての鍵は共に復号化ユニット（DeCryption Unit）に送られ、復号化されて送信相手名が得られる。この送信相手名は、ピース番号処理装置（Piece Number Manegement Unit）に入力され、ピース番号表(Piece Number Table)を参照して、送受信者が共通に持つピースの番号(Common Piece Number)を求める。共通ピース番号は、平文用の暗号化ユニットに入力されて、ここで暗号化され、最後に全てのピース番号を付加されて回答文（answer）となる。

第１１図には、暗号化処理を示す。

システムは、受け取った回答を全てのピース番号と、暗号化された共通ピース番号（ Ciphered Common Piece Number)に分離し、全てのピース番号を利用して生成した鍵を用い、暗号化された共通ピース番号を復号化し、共通ピース番号を得る。このようにして得られた共通ピース番号はピース処理装置に入力されて、送信者と受信者に共通するピース（Common Piece）が得られる。共通ピースは、通信鍵生成装置に送られ、ここではじめて同報通信用の通信鍵Ｋが生成される。この鍵を用いて平文用の暗号化ユニットで、平文を暗号文にする。生成された暗号文には共通ピース番号が暗号化された鍵修正番号として付加されて同報通信文となり、通信回線上に送られる。

最後に、復号化処理のシステムを示す（第１２図）。

システムは、受け取った同報通信文を共通ピース番号と暗号文に分離し、共通ピース番号を利用して通信鍵Ｋを生成し、この鍵を用いて暗号文を平文に復号化する。

（発明の効果）

この発明によれば、同報通信ネットワークのメンバーが所有する第１の鍵を鍵生成手段に入力することによって、通信用鍵となる第２の鍵を生成することができるので管理すべき鍵の数が著しく減少して鍵の管理を簡易、かつ容易化すると共に、漏洩時の被害を最少限度に止め得る効果がある。

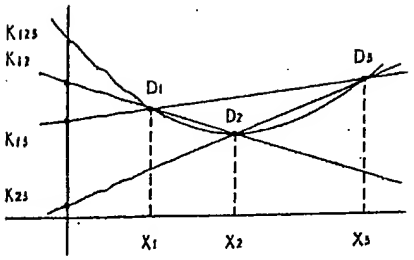
またこれを階層構造の通信に応用した場合においても、鍵とピースの管理の為に安全性が著しく高くなり、ピース自体に直接加工できないような環境を生成することによって、安全性を更に向上することができる効果がある。また、階層構造においては、階層間の通信を実用上制限できるので（例えば社長は部長まで直接通信）、此の点からも管理すべき鍵数を激減することができると共に、通信構成の変更など（例えば人事移動）に際し、柔軟に、速かな対応ができる等の諸効果がある。

4．図面の簡単な説明

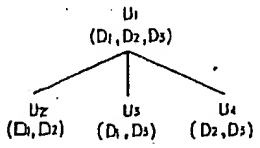
第１図はこの発明に使用するラグランジュ補間方式のグラフ、第２図は同じく２階層構造図、第３図は同じく３階層構造図、第４図は同じくピース番号管理系統のブロック図、第５図は他の発明の情報分配の例示図、第６図は同報通信文の構造を示すブロック図、第７図および第８図は同報通信システムのブロック図で、第７図はメンバー氏名を得てからメッセージ作成までのブロック図、第８図はメッセージを入力してから原文作成までのブロック図、第９図乃至第１２図は階層通信システムのブロック図で、第９図は通信相手名を得てから問合せ文作成までのブロック図、第１０図は問合せ文の入力から回答文作成までのブロック図、第１１図は回答文からメッセージ作成までのブロック図、第１２図はメッセージ入力から原文作成までのブロック図である。

特許出願人　エスアール総研株式会社
同　松下　温
同　岡田　謙一
代理人　鈴木　正次

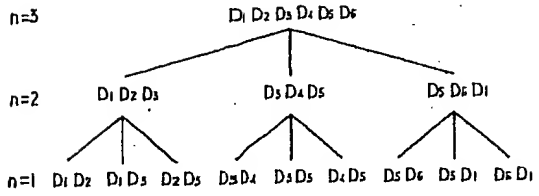
## 第 1 図



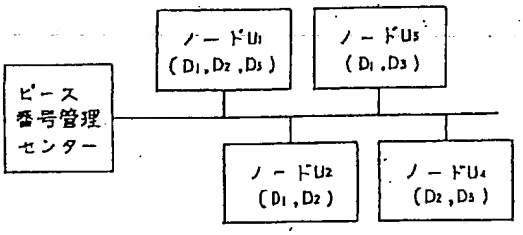

## 第 2 図




## 第 3 図




## 第 4 図

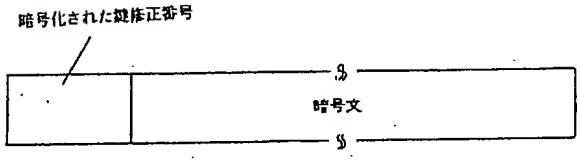



## 第 5 図

| | I1 | I2 | I3 | I4 | I5 | KD |
|---|---|---|---|---|---|---|
| * U1 | ● | ○ | ○ | ● | | ○ |
| U2 | ○ | ○ | ○ | | ○ | ○ |
| * U3 | ● | ○ | | ● | ○ | ○ |
| * U4 | ● | | ○ | ● | ○ | ○ |
| U5 | | ○ | ○ | ○ | ○ | ○ |

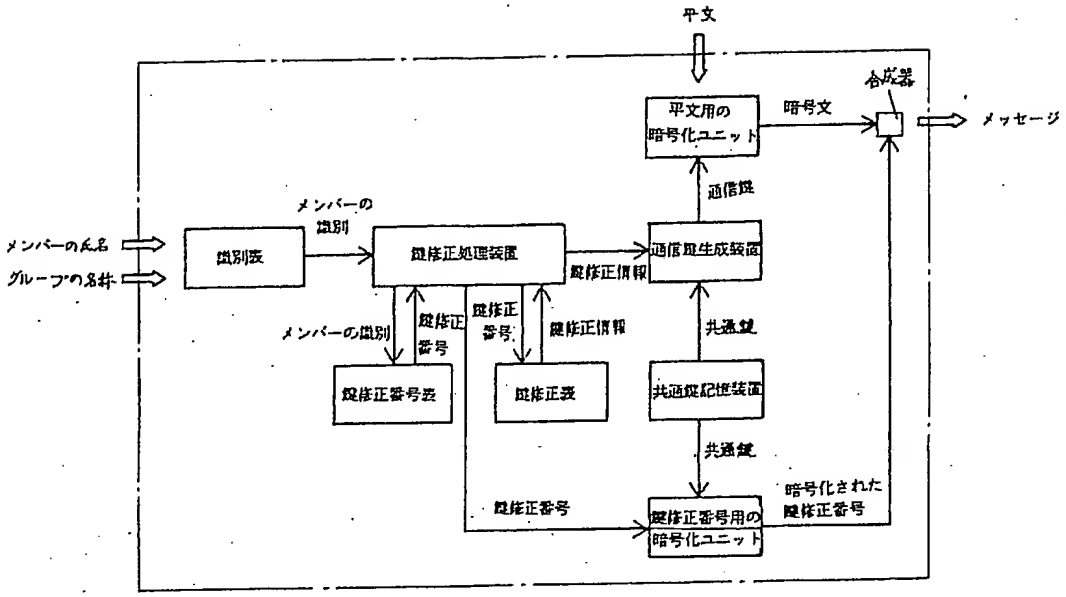
*: グループ {U1, U3, U4} のメンバー
○: 分配されているIKG, または共通キー
●: グループ内で共通のIKG

## 第 6 図

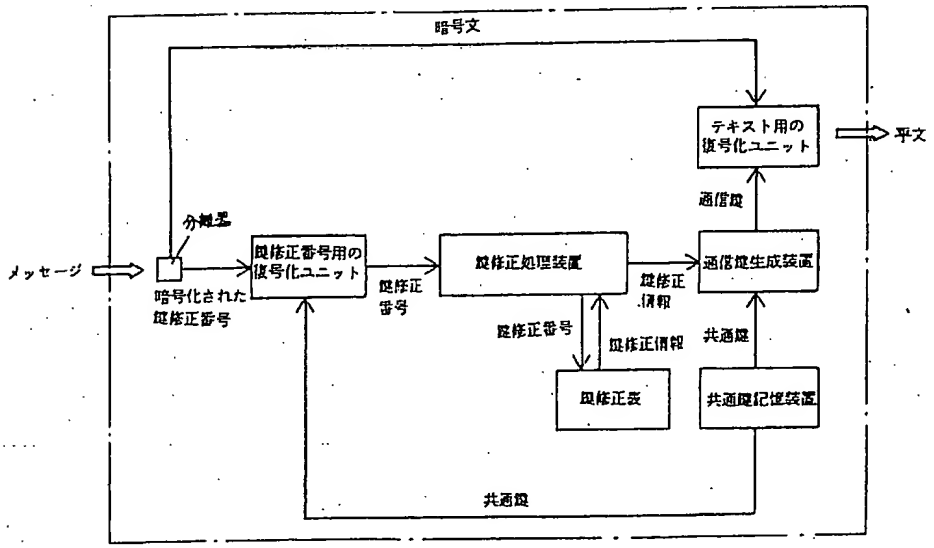



同報通信文のデータ長

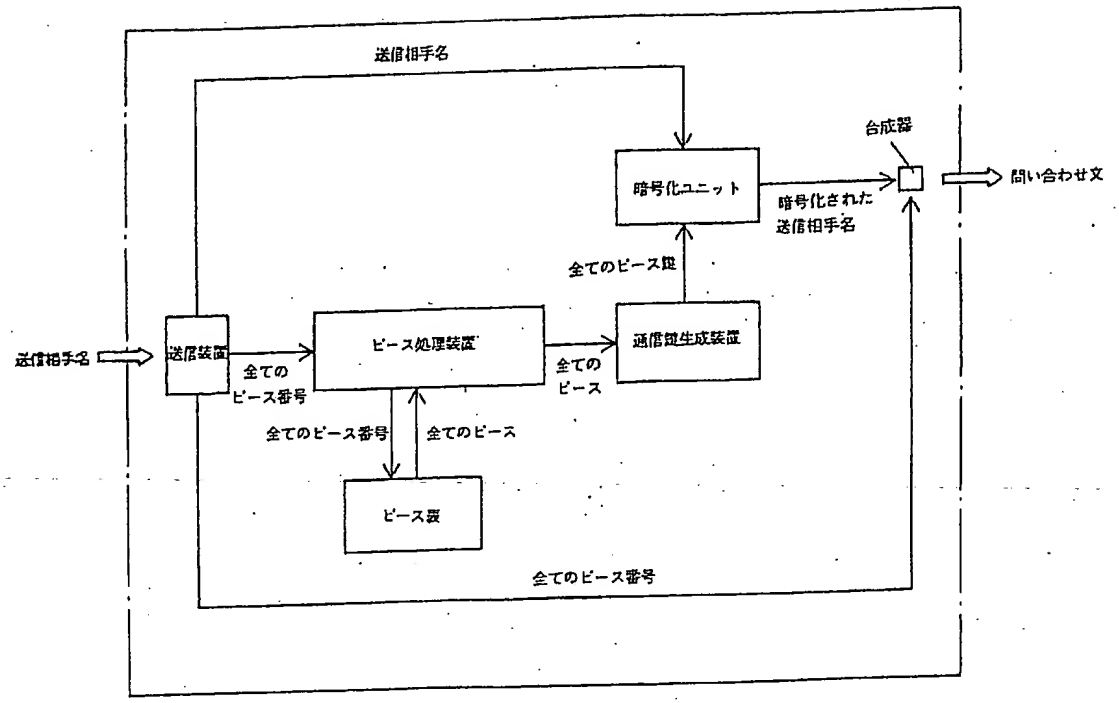
第 7 図


平文
合成器
平文用の暗号化ユニット
暗号文
メッセージ
通信鍵
メンバーの識別
メンバーの氏名
グループの名称
識別表
鍵修正処理装置
通信鍵生成装置
鍵修正情報
メンバーの識別
鍵修正番号
鍵修正番号
鍵修正情報
共通鍵
鍵修正番号表
鍵修正表
共通鍵記憶装置
共通鍵
暗号化された鍵修正番号
鍵修正番号
鍵修正番号用の暗号化ユニット

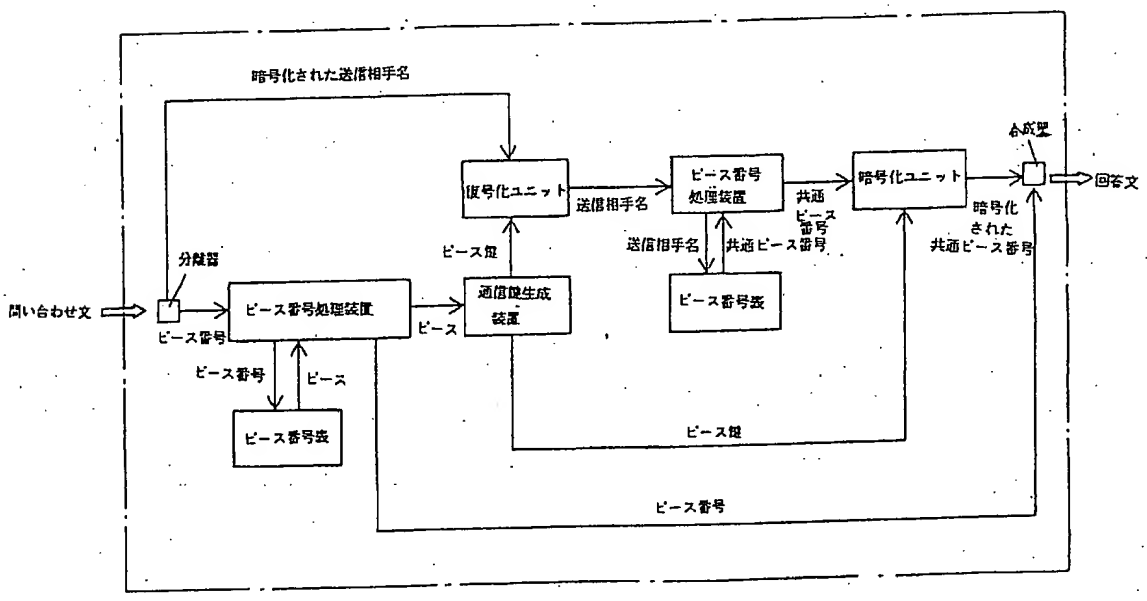
第 8 図


暗号文
テキスト用の復号化ユニット
平文
通信鍵
分離器
メッセージ
鍵修正番号用の復号化ユニット
鍵修正処理装置
通信鍵生成装置
暗号化された鍵修正番号
鍵修正番号
鍵修正情報
鍵修正番号
鍵修正情報
共通鍵
鍵修正表
共通鍵記憶装置
共通鍵

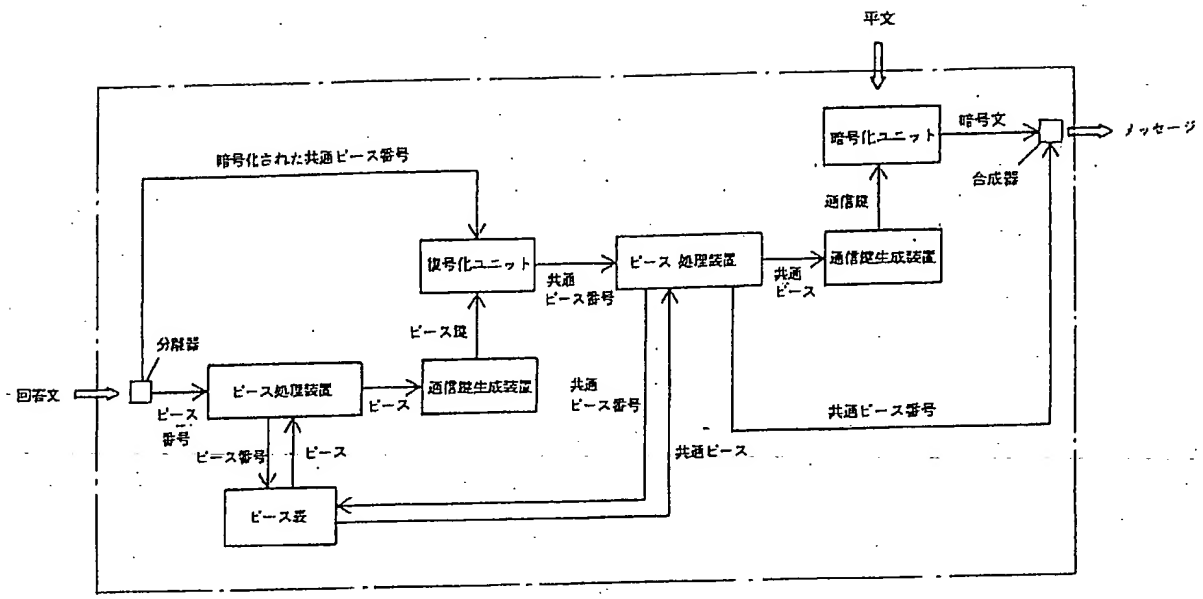
第 9 図


送信相手名
合成器
暗号化ユニット
問い合わせ文
暗号化された
送信相手名
全てのビース鍵
送信相手名
送信装置
全ての
ビース番号
ビース処理装置
全ての
ビース
通信鍵生成装置
全てのビース番号
全てのビース
ビース表
全てのビース番号

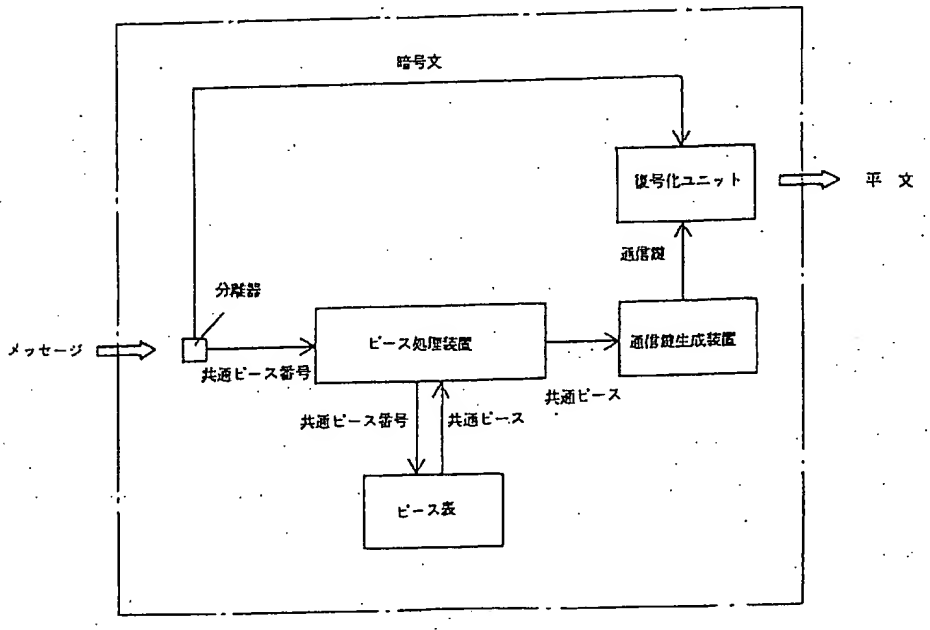
第 10 図


暗号化された送信相手名
合成器
復号化ユニット
ビース番号
処理装置
暗号化ユニット
回答文
送信相手名
共通
ビース
番号
暗号化
された
共通ビース番号
ビース鍵
送信相手名
共通ビース番号
分離器
問い合わせ文
ビース番号処理装置
通信鍵生成
装置
ビース番号
ビース
ビース番号
ビース
ビース番号表
ビース鍵
ビース番号

第11図


平文
暗号化ユニット
暗号文
メッセージ
合成器
暗号化された共通ピース番号
通信鍵
復号化ユニット
ピース 処理装置
通信鍵生成装置
共通
ピース番号
共通
ピース
ピース鍵
分離器
回答文
ピース処理装置
通信鍵生成装置
ピース
ピース
番号
ピース番号
ピース
共通
ピース番号
共通ピース番号
共通ピース
ピース表

第12図


暗号文
復号化ユニット
平 文
通信鍵
分離器
メッセージ
ピース処理装置
通信鍵生成装置
共通ピース番号
共通ピース
共通ピース番号
共通ピース
ピース表